Lightning Talk 5: Detailed Design

SDmay25-07: Ask Captain Cyber

Client & Advisor: Doug Jacobson

Ask Captain Cyber Project Overview

Ask Captain Cyber is a cyber-security focused chatbot that will be able to answer user's questions relating to cybersecurity, with support for all levels of complexity. Questions that have not already been answered will be generate by an LLM and vetted by experts to ensure accuracy.

Detailed Design and Visuals

- Figure 1 details the flow of different user-dependent screens for Ask Captain Cyber
- Access control across different user types
- Streamlined site navigation
- Usability study upon implementation

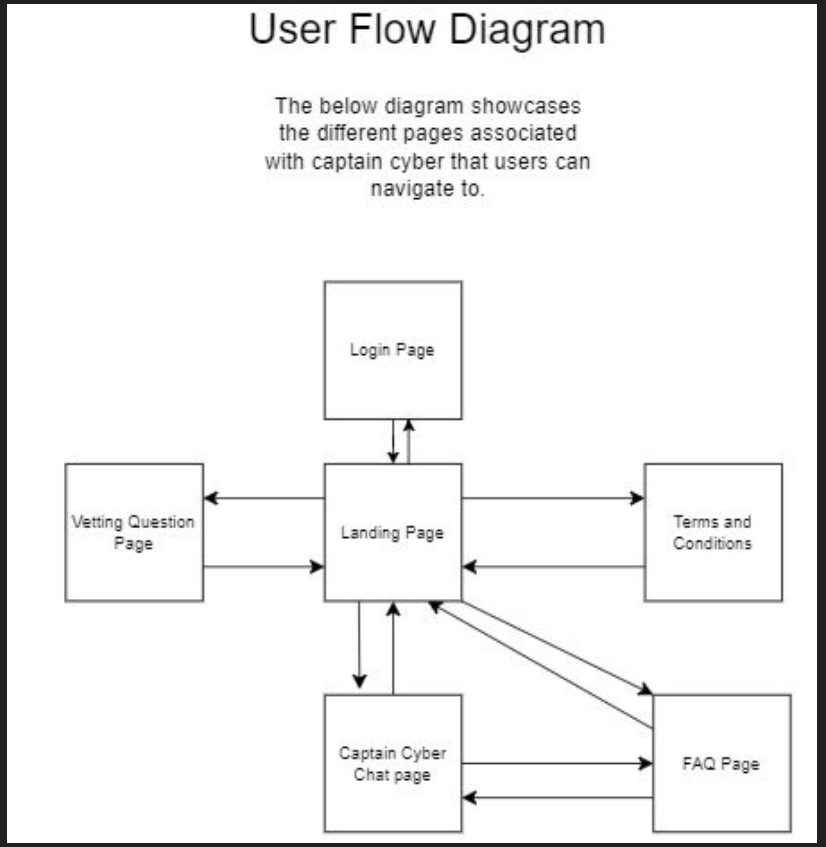

Figure 1: UI Interaction of “Ask Captain Cyber” Webpages

Functionality

- Figure 2 details the control flow of the Ask Captain Cyber application
- Prompt - dependent routes and program behavior
- FAQ database access to minimize time spent waiting for answers

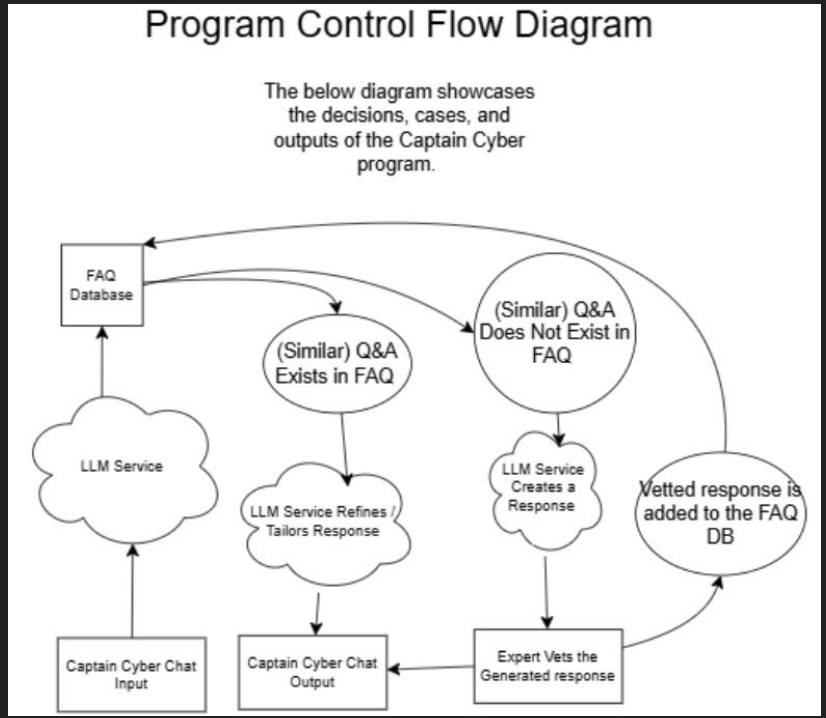

Figure 2: Program Control Flow Diagram

Technology Considerations

Cloud Management Options (Data storage and Processing power)

- ISU resources
- Outside cloud management (within budget)

Backend

- The OS the server uses
- Any networking requirements between AI and data storage?

AI Licenses

- Microsoft Copilot

Areas of Concern and Development

- Login page & database security vulnerabilities
  - SQL & Script Injections
  - Unhashed passwords
- Malicious AI Input
  - Inappropriate questions & responses
  - Personal Information (Socials, Passwords, etc…)
- Multiple users accessing the AI
- Complex Hybrid AI development, with AI and internal LLM along with vetting questions.
- Adhering to ISU standards and potential integration.

Conclusion

In conclusion, the Ask Captain Cyber project is in a good state:

- We have a secure planning foundation on which to build the application
- The required Ask Captain Cyber webpages are under development
- The program control flow is determined; allows ease of development
- We have finalized the technologies we will be using
- The potential risks have been considered; will develop accordingly